REMARKS

In the aforementioned Office Action, claims 1-44 were examined. Claims 1-42 and 44 were rejected and claim 43 was objected to. In view of the following remarks, Applicants respectfully request reconsideration of the application.

Claim Objection

On page 2 of the Office Action, claim 36 stands objected to under 37 CFR 1.75(c) as being of improper dependent for failing to further limit the subject matter of a previous claim. Applicants elect to amend the claim to place the claim in proper dependent form.

Claim Rejection - 35 USC. §112

On page 2 of the Office Action, claim 36 stands rejected under 35 U.S.C. 112, first paragraph. The Examiner asserts, " because the specification, while being enabling for permitting access from any of the locations (Fig. 5F), does not reasonably provide enablement for 'wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers'." The Examiner questions "where control of the access is located, at the client or the server". The Examiner further asserts that the "disclosure does not disclose that the system controls the number of servers that a user gains access [to], instead the disclosure discloses the control of the location that the user can access from." Applicants respectfully traverse.

Applicants have amended claim 36 for clarification. Applicants respectfully submit that support for claim 36 is provided in the text of the specification, as well as the figures. Specifically, Applicants direct Examiner's attention to paragraphs 120-123 and FIG. 5A,C,D,E. The specification discloses that in exemplary embodiments,

control of the access may be located at the central server or any of a number of local servers. "As shown in FIG. 5C, the local server device 570 also executes a module, referred herein as a local module 572 which is configured to be a complete or partial replication of the server module 502 of FIG. 5A." (See paragraph 120 lines 5-7) Moreover, ". . . not all authentication requests need to be handled at one central point . . .a number of local servers are used and each has replication of the server module . . ." (See paragraph 120 lines 14-18)

Contrary to the Examiner's assertion, a careful review of the specification discloses that the specification does discuss both the location and the number of servers that the user can gain access from. For example, the specification supports a "dynamic configuration mechanism" that provides "that secured documents can be accessed by [a user] from only one location at a time". See paragraph 122 lines 7-9. Thus, in various embodiments, a person cannot "log into [a] system or . . . access secured documents from two physical locations at the same time." This is because "for security reasons, it is preferably [sic] that a user, regardless of his/her access privilege, be permitted only a single access location at all times." (See paragraph 122, line 10-13).

Applicants respectfully submit that a careful reading of the text in light of the figures shows that claim 36 is enabled by the specification.

Double Patenting

On page 3 of the Office Action, claims 36-39 stand provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-4 of copending Application No. 10/076,181. The conflicting claims were, however, canceled from copending Application No. 10/076,181 in a response filed on November 21, 2005 to an unrelated Office Action regarding that application. As such, the double patenting rejection is moot.

Claim Rejections - 35 USC §102

On page 4 of the Office Action, claim 36 stands rejected under 35 U.S.C. 102(b) as being anticipated by *Stallings* (Cryptography and Network Security). Examiner asserts that "*Stallings* teaches the Kerberos system comprising: a central server having a server module that provides overall access control (Kerberos authentication server page 333); and a plurality of local servers, each of said servers including a local module that provides local access control (last paragraph on page 333), wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (Kerberos authentication server Fig 11.2)." Examiner further asserts that that *Stallings* teaches the Kerberos system "wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers (page 336 Session keys)." Applicants respectfully traverse.

A careful review of *Stallings* at page 333 discloses that access control is not performed by the central server or the local servers. "The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the Kerberos server. The Kerberos server must share a secret key with each server. " (*Stallings* at page 333 lines 4-8) Thus, the central (Kerberos) server and the local server (user) are both required to perform access control and permit or deny access requests to secured items by requestors.

In contrast, the embodiment of claim 36 provides that access control may be "performed by said central server or said local servers." Thus the local servers may operate to permit or deny access to requests to secured items by requestors, for example, in the absence of the central server. Thus, "not all authentication requests need to be handled at one central point without losing control of the access control

management. As another feature of the present invention, the users are not affected if the central server is brought down for maintenance and the connection to the central server is not available." (See specification paragraph 120 lines 10-14)

Furthermore, a careful review of *Stallings* at page 336-337 discloses that the "Session keys" are intended to prevent serial access (in the time domain). "A new access by the client would result in the use of a new subsession key." (*Stallings* p 337 lines 1,2) There is, however, no teaching that the "Session keys" prevent simultaneous (i.e., parallel) access to secured items from two different servers (local or central) by the same requestor. That is, *Stallings* does not teach that the "Session keys" limit a given requestor (who may be permitted to access secure items through more than one of the local servers) to accessing "secured items using only a single one of the local servers or the central server such that the given requestor can only access secured items through at most one of the local servers at a time." For these reasons, Applicants respectfully submit that *Stallings* does not anticipate claim 36.

Because claims 37-44 depend directly or indirectly from claim 36 these claims are not anticipated for the same reasons as that of claim 36.

Claim Rejections - 35 USC §103

Claims 1-35

On page 5 of the Office Action, claims 1-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Samson* et. al (6,339,423) in view of *Boebert* et al (5,502,766). In reference to claims 1 and 34, Examiner asserts that *Samson* discloses a system and method comprising all the elements of claims 1, and 34 except "authenticating the first client machine." Examiner asserts that *Boebert* discloses the missing element in a system that "comprises an identification and authentication process for the user and the client machine (column 4 lines 26-35)." Examiner asserts that "it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user," and "[o]ne

of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only from terminals located inside the engineering area." Applicants respectfully traverse.

A careful review of *Samson* reveals that *Samson* teaches away from using an identification and authentication process for the user and the client machine. *Samson* discloses a system where a user authentication is stored in a "cookie". The cookie may be presented, by any of multiple client computers where a Multi-Domain Token Server may reside, upon request from a Secondary Domain Agents for access to secured resources. Restricting access to both an authenticated user and a single client computer would defeat the ability of the network to process a request from a Secondary Domain Agent. For example *Samson* discloses,

> "[f]or purposes of efficiency and failure handling, it may be desirable to execute replicas of Multi-Domain Token servers. The access control cookies could be replicated in each Multi-Domain Token Server replica. Thus, when a Multi-Domain Token Server receives a request to store access control cookies, it stores and communicates them to the other Multi-Domain Token Server replicas. Consequently, for the purposes of retrieving access control cookies, a Secondary Domain Agent may request a copy of a set of access control cookies from any replica." (See column 9 lines 31-40)

Thus, there is no motivation by a person of ordinary skill in the art implementing the system of *Samson* to restrict authentication to both a user and a client server as it would defeat the flexibility in the system of *Samson*. As such, there is no suggestion or motivation to combine *Sampson* with *Boebert*. Applicants respectfully submit that independent claims 1 and 34 are not obvious over *Samson* in view of *Boebert*. Because claims 2-20 depend from directly or indirectly claim 1, these claims are not obvious for the same reasons as that of claim 1.

Claims 21 and 35

In reference to claims 21 and 35, on page 6 of the Office Action, Examiner repeats arguments set forth above for claims 1 and 34. Additionally, Examiner asserts that *Samson* discloses a system and method including "retrieving access privileges associated with the user (column 5 lines 38-46)." Applicants respectfully traverse.

As set forth above in regard to claims 1 and 34, *Samson* does not teach using an identification and authentication process for the user and the client machine. Furthermore, a careful review of all occurrences of the term "Multi-Domain Token" in *Samson* reveals that *access privileges associated* with the user are *not available* in the Multi-Domain Token for retrieval. The Multi-Domain Token merely authenticates or identifies the user. For example, "A Multi-Domain Token is an encrypted data item used to verify that the user has been authenticated by Access Control System . . ." (column 5 lines 41-43)

In a further example, "[a]t step 436, [t]he Multi-Domain Token Server 208 determines whether or not the Multi-Domain Token is authentic, that is, whether it had been issued by a Multi-Domain Token Server 208 server for an authentic user." (column 8 lines 38-44)

Therefore, *Samson* does not disclose an identification and authentication process for the user and the client machine. Moreover, there is no motivation to combine the system of *Boebert* with the process of Sampson.

Even if, for the sake of argument, there were motivation to combine the system of *Boebert* with the process of Sampson, *Samson* does not teach "retrieving access privileges associated with the user." The addition of *Boebert* does not cure this deficiency. Therefore, applicants respectfully submit that claims 21 and 34 are patentable over *Samson* in view of *Boebert*.

Because claims 22-33 depend from directly or indirectly claim 21, these claims are not obvious for the same reasons as that of claim 21.

Conclusion

Based on the above remarks, Applicants believe that the rejections in the Office Action of October 6, 2005 are fully overcome, and that the application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicants' undersigned representative at the number given below.

Respectfully submitted,

Klimenty Vainstein et al.

Date: 4/6/06   By: _Susan Yee_

Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444